Omxus: A Sovereign Infrastructure for Direct Democracy and Universal Justice

January 2026

Abstract

A sovereign digital infrastructure is proposed that eliminates intermediary governance through direct democratic participation, prevents crime through universal voluntary response networks, and ensures justice through structural accountability rather than punitive enforcement. The system employs a non-transferable identity token anchored to physical NFC hardware, with sybil resistance achieved through in-person vouching by existing participants. Network resilience is provided through mesh topology operating independently of centralised internet service providers, with cryptographic anchoring to the Bitcoin network via RGB protocol. The architecture embodies four principles derived from medical ethics: autonomy, non-maleficence, beneficence, and justice defined as prevention only.

1. Introduction

Contemporary governance systems operate through representative intermediaries who concentrate decision-making power in institutions vulnerable to capture, corruption, and unilateral action against the interests of constituents. The dismissal of the Whitlam government in Australia (1975) demonstrates the structural fragility of representative democracy: a single unelected actor terminated an elected government without consultation, communication, or recourse. The population had no mechanism to respond.

Modern digital infrastructure compounds these vulnerabilities. Internet access depends on corporate intermediaries (ISPs) operating under state jurisdiction. Identity verification requires centralised authorities. Communication channels can be severed. The technical architecture of contemporary society enables the same pattern: isolate, then act.

Meanwhile, commercial platforms demonstrate that frequent, large-scale coordination is technically feasible. Social networks coordinate billions of daily interactions. Yet governmental democratic participation remains constrained to infrequent elections, with policy decisions delegated to representatives whose expertise rarely matches the domains they govern.

This paper proposes Omxus: infrastructure for direct democratic governance, crime prevention through universal voluntary response, and dispute resolution through mandatory perspective exchange. The system requires no trusted intermediaries, operates on mesh networks independent of ISP infrastructure, and anchors identity and decisions to the Bitcoin blockchain via RGB protocol.

2. Foundational Principles

The system architecture derives from four principles established in medical ethics, adapted for governance infrastructure:

Autonomy. Self-sovereign identity. Individuals control their own cryptographic keys, data, and participation. No entity can revoke identity or access without consensus of the vouching network.

Non-maleficence. The system cannot be weaponised against its participants by design. No surveillance apparatus. No punishment infrastructure. No mechanism exists within the protocol to harm users.

Beneficence. Access to information, communication, and democratic participation as baseline rights. The network exists to serve human flourishing.

Justice (prevention only). No punitive architecture. The system prevents harm through structural design and universal witness, not through punishment after the fact. Justice is redefined as the prevention of injustice, not retribution for it.

3. Identity Layer

3.1 The Omxus Token

Each participant holds exactly one non-transferable token representing verified human identity. The token is not currency; it is proof of personhood and membership in the network. One human, one token. The token cannot be bought, sold, or delegated.

The token is anchored to a physical NFC ring worn by the participant. The ring stores the private key for the participant's decentralised identifier (DID). All actions requiring identity verification—voting, emergency response activation, dispute registration—require physical presence of the ring.

3.2 Sybil Resistance Through In-Person Vouching

The central problem of decentralised identity is sybil resistance: preventing one human from creating multiple identities. Existing solutions rely on biometrics (centralised storage vulnerabilities), proof-of-work (plutocratic), or trusted authorities (single points of failure).

Omxus employs a web-of-trust model with physical verification. To receive a token, a prospective participant must be vouched for by three existing token holders. Vouching must occur in person, with physical co-presence verified through device proximity (NFC handshake, QR code exchange, or equivalent).

The vouching event is recorded as a signed attestation from each voucher, timestamped and eventually anchored to Bitcoin. Vouchers accept ongoing responsibility: if a vouched participant is demonstrated to be a sybil (same human holding multiple tokens), the vouchers' reputation is affected proportionally.

3.3 Genesis Ceremony

The network bootstrap requires an initial set of participants who cannot be vouched for by existing members (as none exist). The genesis ceremony addresses this through collective attestation.

Three initial vouchers assemble nine prospective participants. The ceremony is filmed, with each participant's face, ring, and public key visible. The video is hashed and anchored to the Bitcoin blockchain. This hash becomes the root of the social contract—publicly verifiable, immutable, and tied to identifiable humans who have staked their reputations on the network's integrity.

Subsequent participants are vouched through the standard three-voucher process, creating an expanding web of trust rooted in the genesis event.

4. Direct Democracy

4.1 Elimination of Representative Intermediaries

Representative democracy emerged from communication constraints: citizens could not practically participate in every decision, so they delegated authority to representatives. These constraints no longer exist. Digital infrastructure enables real-time, large-scale coordination.

Omxus eliminates the politician as a role. Policy decisions are made directly by affected participants. Technical implementation is delegated to domain experts (engineers build roads, medical professionals design health policy) who are accountable to direct democratic oversight, not electoral cycles.

4.2 Continuous Participation

Voting occurs continuously, not at fixed intervals. Participants may vote on any active proposal at any time. Proposals have defined windows, but participation is asynchronous—votes are cast when convenient, signed locally, and propagated through the mesh network.

Votes are cryptographically signed by the participant's ring, timestamped, and stored locally before network propagation. This ensures votes cannot be lost to connectivity failures. When the device eventually reaches another node (through mesh, internet, or physical proximity), votes propagate through the network and eventually anchor to the Bitcoin blockchain via RGB.

4.3 Local Meetings

Digital participation is supplemented by physical assembly. Local meetings provide space for deliberation that text-based systems cannot replicate. Participants gather to discuss proposals, hear perspectives, and form considered opinions before casting votes.

Meeting attendance is recorded through NFC proximity verification among attendees, creating a record of deliberative participation without mandating specific outcomes.

5. Crime Prevention Through Universal Response

5.1 The Prevention Principle

Contemporary justice systems are primarily punitive: harm occurs, then the system responds with punishment intended to deter future harm. This approach fails empirically (recidivism rates demonstrate limited deterrent effect) and ethically (punishment does not undo harm to victims).

Omxus inverts this model. Justice is prevention only. The system is designed such that harmful actions cannot occur, or are interrupted before completion, rather than punished afterward.

5.2 Universal Voluntary Response Network

All token holders agree, as a condition of participation, to respond to emergency activations within their proximity. This mirrors the volunteer firefighter model common in regional areas: community members who maintain normal occupations but respond when needed.

When a participant activates an emergency through their ring, all nearby token holders are notified. The density of the network ensures rapid response: if every person is a potential responder, response time approaches zero.

This creates structural prevention: the commission of harm requires isolation of the victim from witnesses and responders. Universal network participation eliminates this isolation. Crime becomes impractical not because punishment is severe, but because completion is impossible.

5.3 Accountability Without Punishment

Actions within the network are cryptographically signed. Participants cannot deny actions they have taken (non-repudiation). This creates accountability through transparency: the truth of what occurred is structurally guaranteed, eliminating disputes of fact.

Where harmful intent is demonstrated, the response is not punishment but intervention: mandatory participation in ViewSwap (Section 6), community

support for addressing underlying causes, and if necessary, restriction of network privileges through voucher consensus.

6. ViewSwap: Dispute Resolution Through Perspective Exchange

6.1 Mechanism

When disputes cannot be resolved through deliberation, participants engage in ViewSwap: a mandatory exchange of circumstances for a defined period (typically one week). Each party lives the other's life—their home, their routine, their constraints.

The mechanism is designed to create embodied understanding that argument cannot achieve. Most disputes arise from failures of empathy—inability to comprehend the other party's constraints, pressures, and perspective. ViewSwap makes this comprehension unavoidable.

6.2 Deterrent Effect

ViewSwap functions primarily as deterrent. The obligation to experience another's circumstances discourages frivolous disputes and incentivises good-faith resolution before escalation. Participants approach conflicts knowing they may be required to inhabit the other party's position.

This deterrent aligns with the prevention principle: ViewSwap prevents intractable conflict by making the cost of intractability personal and immediate, rather than punishing conflict after social harm has occurred.

6.3 Obligation and Duty

Participation in ViewSwap when triggered is a non-negotiable obligation of token holding. This duty is accepted at the moment of vouching and cannot be subsequently declined. The network depends on mutual commitment to perspective exchange as the ultimate dispute resolution mechanism.

7. Technical Architecture

7.1 Network Layer

The network operates on Yggdrasil, an encrypted IPv6 mesh network. Each device receives a cryptographic address and routes traffic through available paths—internet where available, direct device-to-device connections where not. The network self-heals around failures and cannot be disabled through any single point of control.

Peer discovery employs Hyperswarm, enabling devices to locate each other and establish connections through firewalls and network address translation. Participants with internet access serve as gateways to the broader network for those without, distributing access rather than concentrating it.

7.2 Data Layer

Data synchronisation employs Hypercore, an append-only log structure enabling offline-first operation. Participants create signed records locally; records propagate through the network as connectivity allows. Conflict-free replicated data types (CRDTs) ensure that devices synchronising after periods of disconnection merge state deterministically without central coordination.

Critical records (votes, identity attestations, dispute records) are periodically anchored to the Bitcoin blockchain via RGB protocol. RGB enables smart contract functionality on Bitcoin's UTXO model without requiring a separate blockchain or token. Anchored records are immutable and independently verifiable by any party with Bitcoin access.

7.3 Identity Layer

Identity employs W3C Decentralised Identifiers (DIDs). Each participant controls a DID anchored to their NFC ring's secure element. The ring stores the private key; the public key and attestations are distributed through the network.

Authentication requires physical ring presence. No passwords, no centralised identity providers, no CAPTCHAs. Identity is proven through cryptographic signature from a key that requires physical hardware to access.

7.4 Resilience Properties

The architecture provides resilience against the failure modes that enable authoritarian intervention:

No ISP kill switch: mesh routing bypasses centralised infrastructure. No server to seize: data is replicated across all participants. No database to corrupt: each participant maintains an independent copy, with Bitcoin anchoring providing ultimate verification. No company to pressure: no legal entity operates the network. No identity to revoke: DIDs are self-sovereign and cannot be disabled by external authority.

8. Economic Implications

8.1 Elimination of Administrative Overhead

Contemporary governance requires substantial bureaucratic infrastructure: election administration, legislative staffing, regulatory agencies, justice system personnel. Omxus replaces these functions with protocol—automated, transparent, and requiring no ongoing administrative labour.

Australia allocated approximately $32 billion to justice administration in 2019. The majority of this expenditure addresses functions that Omxus renders unnecessary: dispute adjudication (replaced by ViewSwap), crime response (replaced by prevention), incarceration (eliminated by the prevention principle). These resources become available for direct human benefit.

8.2 Reclaimed Time

A substantial portion of contemporary labour serves administrative rather than productive functions: compliance, reporting, verification, authentication. Omxus eliminates much of this through cryptographic proof: identity is proven by ring, actions are verified by signature, compliance is ensured by protocol.

The elimination of administrative friction, combined with direct democratic efficiency, enables substantial reduction in required labour. Participants may find themselves with significantly increased discretionary time—potentially twenty or more hours per week—to allocate according to their own values.

9. Conclusion

Omxus proposes infrastructure for a fundamentally different social organisation: one where governance is direct, justice is preventive, and access is universal. The technical components—mesh networking, decentralised identity, blockchain anchoring—are not novel individually. The contribution is their composition into a coherent system embodying specific ethical principles.

The system requires no trusted intermediaries. It cannot be disabled by authoritarian action. It provides every participant with equal voice in collective decisions and equal protection through universal response.

The goal is not utopia but robustness: a social infrastructure that cannot be Whitlam'd. Where no one can be isolated, silenced, or overruled by unilateral action. Where eight billion humans have access to communication, information, and collective self-determination as basic rights rather than privileges granted by intermediaries.

Autonomy. Non-maleficence. Beneficence. Justice.

Prevention only.